

Express Mail No. EL655493071US  
FILE NO. ATTA-25,441

**SYSTEM AND METHOD FOR TRANSMISSION OF INFORMATION  
BETWEEN LOCATIONS ON A COMPUTER NETWORK WITH THE USE OF  
UNIQUE PACKETS**

Inventor(s):

Diane L. Peterson

Patented "Sept 4, 2001"

Express Mail No. EL655493071US

FILE NO. ATTA-25,441

PATENT

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

**SYSTEM AND METHOD FOR TRANSMISSION OF INFORMATION  
BETWEEN LOCATIONS ON A COMPUTER NETWORK WITH THE USE OF  
UNIQUE PACKETS**

**TECHNICAL FIELD OF THE INVENTION**

**[0001]** This invention is related to data processing systems and their architecture. In one aspect, it relates to a network component for retransmitting data packets in accordance with ID codes embedded therein in a distributed manner.

ATTORNEY'S OFFICE

## BACKGROUND OF THE INVENTION

[0002] The classification and management of data is one of the most difficult tasks faced by corporations, government entities, and other large users of information. Companies must classify their data in such a way to make it easy and simple for buyers to find and purchase their products. Data exchanges face a bigger challenge in that they must work with multiple companies and develop a comprehensive classification system for their buyers.

[0003] One common way to create a search/classification system for specific products is to access and use government and/or industry specific classification systems (*i.e.*, classification databases). However, no existing classification database is comprehensive enough to address all the issues associated with building a classification system. These issues include: uniform numbers for products that cross multiple industries, restricting products from inclusion in classification, and non-usage of slang or industry standard language to access or classify products. The classification databases frequently do not address all the products, thus resulting in inconsistencies even when companies use the same classification system.

[0004] Additionally, many of the various classification systems conflict with each other. For example, a product might have several classification numbers if it crosses multiple industries. Still other companies might use third party classification systems approved by a governmental entity. This program requires companies to pay multiple fees and go through a lengthy administrative process. Even then it may not cover all products in an industry. Companies must make a conscious decision to initiate, implement and maintain these programs. These efforts can be costly, and for this reason, compliance is generally not high.

[0005] A need therefore, exists, for a data processing system which automatically generates identification codes for specific products. Preferably, companies could use the

automatically-generated identification codes in place of their existing identification codes. More preferably, the use of the automatically-generated identification codes can be phased-in gradually as the of user base expands.

[0006] Under current practices, companies create search engines by developing hierarchies and families of products. They may create a thesaurus to encompass slang words. Companies often use drop down menus, key words and product description capabilities to enhance their systems. It is desired to classify the data in such a way as to minimize the responses generated by a search, and therefore more effectively guide the buyer through the system. However, under current practices, most exchanges offer barely adequate search capabilities for their buyers. Buyers must click through numerous drop down menus and then sort through multiple entries to accomplish their objectives. In many instances the buyer will fail to find the product that they seek. These existing processes could therefore be characterized as cumbersome, time consuming, frustrating and ineffective. A need therefore exists, for a product classification system which can facilitate simple, rapid and effective searching by prospective buyers.

[0007] Another challenging data management task is the transmission of data between dissimilar systems. Even within the same corporate organization it is very common to find different system types, applications and/or information structures being used. Transmitting data between such systems can be a time-consuming and expensive task. Under current practices, data transfer between dissimilar systems is often facilitated by the use of customized software applications known as “adapters”. Some adapters “pull” data, *i.e.*, extract it from the source system in the data format of the host system or host application, convert the data into another data format (e.g., EDI) and then sometimes convert it again into yet another data format (e.g., XML) for transmission to the destination system. Other adapters “push” data, *i.e.*, convert the data from the transmission data format (e.g., XML) to an intermediate data format (e.g., EDI) if necessary, then convert it to the data format of the host system or application at the destination system, and finally loading the data into the destination system. All of these adapter steps are performed on the host systems using

the host systems' CPU. Thus, in adapter-based systems, CPU load considerations may affect when and how often data pulls can be scheduled. For example, data pulls may be scheduled for late nights so as slow down the CPU during daytime ONTP (on line transaction processing). A need therefore exists for a system architecture which can allow the transmission of data between dissimilar systems while minimizing the associated load imposed on the host system CPU.

[0008] Network routers are known which direct data packages on a network in accordance with ID codes embedded in the data packets. However, these routers typically direct data packets between similar nodes on a single network. It is now becoming increasingly common to transmit data across multiple networks, and even across different types of networks. A need therefore exists for a router which can direct data over networks of different types in accordance with associated ID codes. A need further exists for a router which can automatically transform a data packet having a first data format into a second data format.

[0009] It is well known that when large amounts of data are being transmitted between systems, a system error (*i.e.*, stoppage) and/or data loss (*i.e.*, dropout) may occur. With conventional adapter-based system architectures, debugging a system stoppage can be very challenging because of the large number of conversion processes involved, and because most systems do not have an integrated way to indicate the point at which processing stopped, relying instead upon error logs. A need therefore exists for a system architecture in which processing status information is an integral part of the data packets transmitted over the networks.

[0010] Further, with adapter-based systems, even after the processes have been debugged, it is often necessary to wait (e.g., until the time of day when host system CPU demand is low) to replace lost data in order to avoid adverse impact on the company's business. For example, if the host system is used for OLTP (on line transaction processing) during the day, pulling bulk data from the host system in order to replace data lost in a previous data

transfer may be delayed until the late night hours. Of course, the delay in processing the data can have an adverse impact of its own. A need therefore exists for a system architecture which allows for the replacement of lost data while minimizing the impact on the source host system.

## SUMMARY OF THE INVENTION

[0011] The present invention disclosed and claimed herein, in one aspect thereof, comprises a method for communicating between first and second unlike systems. Information is generated at the first system in a first information format that is native to the first system. A first conversion system, in a first conversion operation, converts the generated information to a master space format such that a first converted information transmission is generated. The first converted information is then transmitted to a master information system. In response to receiving the first converted information at the master information system, the received first converted information is routed to a second conversion system in the master system format. At the second conversion system, the information transmitted thereto is converted from the master space format to a second information format in a second conversion operation to provide a second converted information transmission, the second information format being native to the second system. The second converted information transmission is then routed to the second system.

## BRIEF DESCRIPTION OF THE DRAWINGS

[0012] For a more complete understanding of the present invention and the advantages thereof, reference is now made to the following description taken in conjunction with the accompanying Drawings in which:

[0013] FIGURE 1 illustrates an overall diagrammatic view of the system of the present disclosure;

[0014] FIGURE 2 illustrates the detail of flow between elements of the system of the present disclosure;

[0015] FIGURE 3 illustrates the flow of packets between elements in the system and the conversion as the packets flow through the system;

[0016] FIGURES 4A-4D disclose diagrammatic views of the proprietary portion of a transaction packet;

[0017] FIGURE 5 illustrates a diagrammatic view of databases at the host/client and the conversion thereof to a proprietary routing ID packet;

[0018] FIGURE 6 illustrates a diagrammatic view of one instantiation of the system of the present disclosure illustrating a transaction from a first host to a second host or client on the system;

[0019] FIGURES 7A and 7B illustrate two separate channels on the system;

[0020] FIGURE 8 illustrates a flow chart depicting the initial operation of generating the blocks of data for a transaction and scheduling those blocks for transmission;

[0021] FIGURE 9 illustrates a flow chart depicting the data flow analysis operation;

[0022] FIGURE 10 illustrates a diagrammatic view of a transaction table that is formed during the transaction for analysis process;

[0023] FIGURE 11 illustrates a flow chart depicting the export operation wherein the data is polled and transmitted in packets;

[0024] FIGURE 12 illustrates the operation of assembling the data packets;

[0025] FIGURE 13 illustrates a diagrammatic view of a single channel and the processes performed in that channel;



- [0026] FIGURE 14 illustrates a diagrammatic view of two adjacent channels that are utilized in completing a transaction or a process between an origin and a destination.
- [0027] FIGURE 14A illustrates the joiner IDs for the two channels;
- [0028] FIGURE 15 illustrates a schematic diagram of three separate process systems joined by separate channels;
- [0029] FIGURE 16 illustrates a diagrammatic view of the manner in which feeds are propagated along a process chain;
- [0030] FIGURE 17 illustrates the process flow for the feeds in a given process or transaction;
- [0031] FIGURE 18 illustrates a flow chart for the operation at each process node for determining from the feed the process to run and then selecting the next feed;
- [0032] FIGURE 19 illustrates a diagrammatic view of three adjacent channels in a single process flow;
- [0033] FIGURE 20 illustrates a diagrammatic view for a non-system host or origin process node accessing a system process node;
- [0034] FIGURE 21 illustrates the process at the router for handling an out of system process node that originates a transaction;
- [0035] FIGURE 22 illustrates a diagrammatic view of a simplified network for servicing a non-system node with the processes illustrated;
- [0036] FIGURE 23 illustrates an alternative embodiment of the embodiment of FIGURE 22;
- [0037] FIGURE 24 illustrates a more detailed diagram of the data packet;
- [0038] FIGURE 25 illustrates a detail of the preamble of the data packet;
- [0039] FIGURE 26 and 27 illustrate the hierarchal structure of the classification system associated with the data packet;
- [0040] FIGURE 28 illustrates a diagrammatic flow of a classification operation;
- [0041] FIGURE 29 illustrates a flow chart for creating a data packet;
- [0042] FIGURE 30 illustrates a diagrammatic view for associating an input profile with a previous data packet, creating a new data packet;

- [0043] FIGURE 31 illustrates a block diagram for layering of data packets;
- [0044] FIGURES 32 and 33 illustrate block diagrams for two embodiments of a communication system for conversing between two nodes with data packets; and
- [0045] FIGURES 34 and 34a illustrate an example of communication with a data packet.

FIG. 31

## DETAILED DESCRIPTION OF THE INVENTION

[0046] Referring now to FIGURE 1, there is illustrated a system diagram for the presently disclosed system. There are illustrated three transactional systems, 102, 104 and 106. Transaction system 102 is comprised of a router 108 that is interfaced with a network mesh 110, which network mesh 110 is local to the system 102. The network mesh 110 allows the router 108 to interface with various system nodes. There is provided a host system node 114 that is the node at which a transaction arises. Also attached to the network mesh 110 is an archival server 116 and a conversion server 118, the function of which will be described hereinbelow. Since the host system 114, the servers 116 and 118, and the router 108 are all in the same network mesh 110, they communicate in a common protocol to that of the network mesh 110, and also may have the ability to communicate over the network mesh 110 with other network protocols that presently exist and any future protocols that would be developed at a later time. This allows data packets to be transferred between the various nodes on the network mesh 110.

[0047] The router 108 is also provided with various media interfaces 120 and 122. Media interface 120 allows the router 108 to interface with a private network 124 which could be any type of private network such as a local area network (LAN) or a wide area network (WAN). This private network 124 can have other systems attached thereto such that the router 108 can forward data through this network 124. The media interface 122 is interfaced with a global public network (GPN) 126, which is typically referred to as the "Internet." This allows the router 108 to interface with the GPN 126 and the multitude of resources associated therewith, as are well known in the art.

[0048] The system 106 is similar to the system 102 in that it has associated therewith a central router 128. The router 128 is interfaced with a network mesh 130, which network mesh 130 is also interfaced with a universal ID server 132 and a universal web server 134. The router 128 is also interfaced with the GPN 126 with a media interface 136. As such, the router 108 could effectively interface with the router 128 and the network resources in

the form of the universal ID server 132 and the universal web server 134, the operation of which will be described hereinbelow.

[0049] The third system, the system 104, is comprised also of a central router 136, similar to the routers 108 and 128. The router 136 is interfaced on the local side thereof to a local network mesh 138. Local network mesh 138 has associated therewith three host or transaction nodes, a transaction node 140 associated with a system A, a transaction node 142 associated with a system B and a transaction node 144 associated with a system C, the transaction nodes 140-144 all interfacing with the network mesh 138. In addition, the system 104 has associated with its local network mesh 138 a core ID server 146, an account ID server 148, a conversion server 150 and an archival server 152.

[0050] Router 136 is operable to interface with the private network 124 via a media interface 154, interfaced with the GPN 126 via a media interface 156 and also to a transmission medium 158 through a media interface 160. The transmission medium 158 is an application specific medium that allows information to be transmitted to an end user output device 162 through a media interface device 164 or to be received therefrom. As will be described hereinbelow, this end user output device might be a fax machine, and the transmission medium 158 a telephone system or the such that allows data in the form of facsimile information to be transmitted from the router 136 through the transmission medium 158 to the end user output device 162 for handling thereof. The transmission medium 158 may be merely a public telephone network (PTN) that allows the number of the end user output device 162 to be dialed, *i.e.*, addressed, over the network or transmission medium 158, the call answered, a hand shake negotiated, and then the information transferred thereto in accordance with the transaction that originated in the access to the transmission medium 158. The transmission medium could include a satellite transmission system, a paging transmission system, or any type of other medium that interfaces between one of the routers and a destination/source device. This will be described in more detail hereinbelow.

[0051] In addition to allowing the router 136 to directly interface with an end user device 162 via the interface 160, there is also provided a fifth transaction node 166 that is disposed on the GPN 126 and has access thereto via a media interface 168. The transaction node 166 is operable to interface with any of the routers 108, 128 or 136.

[0052] In operation, as will be described in more detail hereinbelow, each of the transaction nodes 114, 140, 142, 144, is able, through the use of the disclosed system, to complete a transaction on the system and utilize the system to send information to or retrieve information from another transaction node on the system. In the private network 124, there is illustrated a phantom line connection between the router 108 and the router 136. In order to facilitate a connection between, for example, transaction node 140 for system A and , for example, transaction node 114 for system D, it is necessary to create a unique data packet of ID's that can be transmitted via the router 136 through the network 124 and to, transaction node 114 for system D. This unique proprietary transaction packet that is transmitted utilizes various distributed resources in order to allow this transaction packet to be processed within the system and transmitted over a defined route that is defined in an initial transaction profile that is stored in the system at various places in a distributed manner. This will be described in more detail hereinbelow. Additionally, the router 136 could also allow one of the transaction nodes 140-144 to interface with the router 108 through the GPN 126 such that a transaction can be completed with the transaction node 114 for system D. This would also be the case with respect to interfacing with the universal ID server 132 or the universal web server 134, the transaction node 166 for system E or with the end user output device 162.

[0053] Each of the routers 108-128 and 136 have associated therewith a data cache 170, 172 and 180, respectively. Whenever a particular router in one of the systems 102-106 has data routed thereto, data may be cached, then processed either outside the system or internal to the system, or the data is maintained in the cache for later transmittal. The general operation of a transaction would require one of the transaction nodes to determine what type of transaction was being made and the destination of that transaction. If it were

determined that the transaction would be between transaction node 140 and transaction node 114 on system 102, a unique transaction packet would be generated that would have unique transaction IDs associated therewith that defined the routing path in the system and the transaction associated therewith while processing what needed to be done between the two transaction nodes. As will be described hereinbelow, this transaction is distributed over the entire system, with only a portion thereof disposed at the transaction node itself. It is the unique transaction codes or IDs that are embedded in the information that is sent to the system that allows the transaction to be carried out in a distributed manner at all of the various elements along the path of the transaction.

[0054] As a further example, consider that transaction node 114 for system D utilizes a different database than transaction node 140, *i.e.*, the two nodes are in general incompatible and require some type of conversion or calculation to interface data and transactional information. With the transaction determined at the transaction node originating the transaction, and a unique transaction packet created with the unique transaction information contained therein, all the necessary information to complete the transaction and the routing of data follows the transaction packet through the system. This, in association with information disposed in other elements or nodes of the system, allows the transaction to be completed in a distributed manner. In particular, the transaction packet is transmitted to various nodes which perform those discrete functions associated with the transaction packet for the purpose of converting, routing, etc. to ensure that the transaction packet arrives at the correct destination and achieves the correct transaction.

[0055] Referring now to FIGURE 2, there is illustrated a diagrammatic view of the system 104 and a transaction between transaction nodes on the network mesh 138, which network mesh 138 is illustrated as a general network. It is noted that network mesh 138 could be any type of network, such as an Ethernet, a satellite, a Wide Area Network or a Local Area Network. The transaction is illustrated as occurring between transaction node 140 for system A and transaction node 142 for system B. Although the details of a transaction will be described in more detail hereinbelow, this transaction is illustrated in

a fairly simple form for exemplary purposes. The transaction is initiated at transaction node 140 to generate information that will be transmitted to transaction node 142 for system B. When the transaction is generated, the type of transaction is determined, the manner in which the information is to be transmitted to transaction node 142 is determined and the route that it will take is determined, and all of the information is embedded in a transaction packet. This is a predetermined transaction that is completed with the use of IDs that are utilized by various systems on the network to appropriately route information and to possibly perform intermediate processes on the packet and the data associated therewith. Further, transaction node 140 has associated therewith information to allow the data that needs to be transferred to be transferred in a predetermined manner in accordance with a known profile of how transaction node 142 wants the transaction to be completed and in what form the data is to be run. For example, it may be that transaction node 140 desires to order a particular product in a particular quantity from transaction node 142. The data associated with the transaction or transactions would be assembled, in accordance with a predetermined transaction profile as determined by the system beforehand and in accordance with a business relationship between the transacting parties, and forwarded to the appropriate location in the appropriate format to be received and processed by transaction node 142. These are transactions that transaction node 140 typically receives and handles in their day-to-day business. As such, all transaction node 142 desires to do is to receive the transaction in a manner that is compatible with its operational environment. By using various conversion algorithms, routing algorithms and the such, the transaction can be effected between the two systems in a distributed manner.

[0056] Although not illustrated in FIGURE 2, and as will be described hereinbelow, there is an initial setup that defines a profile for a transaction and a profile for a transaction node in the system. Whenever it is desirable for transaction node 140 for system A, for example, to create a business relationship with transaction node 142, this business relationship will be set up on the system as a transaction profile. Once the transaction node is set up, the various information that is necessary for the two transaction nodes to converse will be set

up on the system and "propagated" over the system such that the transaction profile is "distributed" about the system. This will be described in more detail hereinbelow.

[0057] In the transaction illustrated, the first step is to create the transaction packet and route it to the router 136. This is facilitated over a path "A" through the network 138. The router 136 is then operable to examine the contents of the transaction packet and the IDs associated therewith with a look-up table (LUT) 202. In the LUT 202, the router 136 determines that this transaction packet is associated with a particular transaction and that the transaction requires that any information for this type of transaction being received from transaction node 140 be transferred to the conversion server 150. The router 136 then reassembles the packet and transfers this transaction packet over the network 138 to the conversion server on a path "B" and also stores the information in its associated data cache. Router 136 has, as such, "handed off" the transaction to the conversion server 150 and then created a record in its local cache 180. (This could be stored in non local cache also, such as at the archive server 152.) It is noted that the transaction packet may be converted at each node along the path, depending upon the transaction and the action to be taken at each node.

[0058] At the conversion server 150, the received packet from the path "B" is examined to determine information associated therewith. The conversion server 150 also has an LUT associated therewith, an LUT 204. The conversion server 150 recognizes that the information came from the router 136 and has a predetermined transaction associated therewith merely from examining the IDs, processing them through the LUT 204 and then determining what type of process is to be performed on the data packet and the contents thereof and where to forward them to. For example, the operation of the conversion server could be as simple as converting the data from an SML language to an XML language, it could be utilized to translate between languages, or any other type of conversion. Primarily, the contents of the transaction packet and associated data that was retrieved from the database associated with transaction node 140, associated with the transaction therein, may require conversion in order to be compatible with the destination transaction node 142.



The conversion server 150 places the data in the appropriate format such that it will be recognized and handled by the transaction node 142. The specific manner by which this conversion is achieved is that setup in the initial setup when the business relationship between the two transaction nodes 140 and 142 was defined. The reason that this particular conversion was performed is that the agreed upon transaction set these parameters in the system for this portion of the transaction which is stored in the LUT 204 at the conversion server 150.

[0059] After the conversion server 150 has processed data in accordance with the transaction IDs within the data packet, the transaction data packet is then reassembled with the destination address of the router 136 and transferred back to the router 136 via a path "C," which may also modify the transaction packet to some extent, as will be described in more detail hereinbelow. Router 136 recognizes this data packet as having come from the conversion server 150 and performs a look-up in the LUT 202 to determine that this particular transaction, determined from the transaction IDs associated therewith, requires data received from conversion server 150 to be transferred to the transaction node 142. The data is then assembled in a transaction packet and transmitted to transaction node 142 along the path "D." Additionally, the previous cached data in cache 180 is replaced by the new data that is forwarded to transaction node 142. In some instances, it is desirable to archive the data associated with this transaction. This is facilitated by the archive server 152, wherein the data transmitted to the transaction node 142 along the path "D" is also transferred to the archive server 152 along a path "D'."

[0060] As will be described hereinbelow, the entire transaction is determined by a unique transaction packet that has embedded therein routing information in the form of ID packets, data, etc. The ID packets are unique numbers that are recognized by each of the nodes in the network to which it is routed. By recognizing an ID packet, the particular router 136, conversion server 150, etc., has information associated therewith that allows it to perform the portion of the transaction associated with that particular node, *i.e.*, the conversion server 150 performs a conversion and then routes it back to the router 136. In this manner, the originating transaction node need not embed all the transaction information therein and

actually effect a direct connection, through a network or otherwise, to the destination transaction node in order to complete the transaction, nor does the originating transaction node require all the transaction information to be associated therewith. As such, the transaction itself is distributed throughout the network in a predetermined manner.

[0061] Referring now to FIGURE 3, there is illustrated a diagrammatic view of the manner in which the packet is modified through the transaction. An originating transaction packet 302 is generated at the originating transaction node 140. This is then transferred to the router 136, wherein the router 136 evaluates the transaction packet, determines where it is to be sent and then converts the packet to a "conversion transaction packet" 304, which is basically the transaction packet that is designated by the router 136 for transmittal to the conversion server 150 via the path "C" with the necessary information in the form of ID packets, data, etc., that will be required by the conversion server 150 to perform its portion of the transaction, it being noted that the transaction packet may undergo many conversions as it traverses through the system. The conversion server 150 then processes the data contained in the conversion transaction packet and then, after processing, converts it to a router transaction packet 306 for transmission back to the router 136. The router 136 then converts this to a destination transaction packet 308 for transmission to the destination. It is noted that the conversion server 150, after receiving the router transaction packet, has no knowledge of where the destination of the transaction packet will be eventually, as it has only a small portion of the transaction associated therewith. All it is required to know is that the transaction packet requires a certain action to be taken, *i.e.*, the conversion process, and then this transaction packet must be transmitted back to the router 136. Since this transaction packet always has associated therewith the necessary ID information as to the transaction, each node that the transaction packet is transferred to or through will recognize where the transaction packet came from, what to do with the transaction packet and then where to transfer it to. Each node then will transfer the transaction packet to the destination eventually in a "daisy chain" manner.

[0062] Referring now to FIGURES 4A-4D, there are illustrated diagrammatic views of the packet transmission which facilitates transmission of a transaction packet between transaction nodes or even nodes in a network. Prior to describing the formation of and transmission of the transaction packet, the distinction must be made between a “data” packet and a “transaction” packet. In general, data is transmitted over a network in a packetized manner; that is, any block of data, be it large or small, is sent out in small “chunks” that define the packet. However, the packet is a sequence of fields that represent such things as headers, footers, error correction codes, routing addresses and the data which is sent as an intact “unit.” Sometimes, the data contained in the packet is actually a small portion of the actual overall data that is to be transmitted during a data transfer operation of some predetermined block of data. These packets typically have finite length fields that are associated therewith and some even have longer variable length fields for the data. However, for large blocks of data, the data will be divided up into smaller sub-blocks that can be sent in each packet. Therefore, for example, a large block of data would be sent to the network controller for transmission over a compatible network to a network controller on a receiving device for assembly thereat. The block of data, if it were large enough not to be compatible with a single data packet, would be divided up into sub-blocks. Each of these sub-blocks is disposed within a data packet and transmitted to the receiving device which, once receiving it, will ensure that this data is then sequenced into a combined block of data. If, for example, one of the data packets had an error in it, this would be communicated back to the transmitting device and that particular data packet possibly retransmitted or the entire block of data retransmitted. Since each data packet has a sequence number when sending a group of data packets that represent one block of data, the individual packets that each contain a sub-block of data can be reassembled to provide at the receiving device the entire packet. This packetising of data is conventional.

[0063] With specific reference to FIGURE 4A, there is illustrated the manner by which the data is actually transmitted. Typically, network controllers are arranged in multiple “layers” that extend from an application layer down to a transport or network layer that inserts the data into a new format that associates a data field 402 with a header 406. The

embodiment of FIGURE 4A is referred to as an IPX data flow controller. As noted hereinabove, whenever a computer is attached to a network, it becomes a node on a network and is referred to as a workstation. When information is sent between the nodes, it is packaged according to the protocol rules set up in the network and associated with the network controller. The rules are processes that must be complied with to utilize the operating system protocol layers - the application layer, the presentation layer, the session layer, the transport layer, the network layer, the data link and the physical layer - in order to actually output a sequence of logical "1's" and "0's" for transmission on the network mesh.

[0064] At the network layer, the data field 402, which was generated at the application layer, is associated with the header 406. This particular configuration is then sent down to the data link which is illustrated as a block 408 which basically associates the data field 402 with a UDP header 410 and then translates this data field 402, UDP header 410 and the IPX header 406 which is then translated into a new data field 412. This new data field 412 at the datalink is then associated with IPX header 414 which is then again converted to a data field 414 associated with a media access controller (MAC) header 416 which is then compatible with the physical layer. The physical layer is the network mesh. This data field 414 and header 416 are what is transferred to the network and what is received by the receiving device. The receiving device, upon receiving the MAC header 416, recognizes an address as being associated with that particular receiving device and then extracts the data field 414 therefrom, which is again utilized to extract the header 414 for examination purposes and, if it is compatible with the device, then the data field 412 is extracted and so on, until the data field 402 is extracted. Of course, data field 402 is only extracted if the data packet comprised of the MAC header 416 and data field 414 is that directed to the particular receiving device. It is noted that all devices on the network mesh will receive the data packet, *i.e.*, they can all "see" the data packet traveling across the network mesh. However, the data will only be extracted by the addressed one of the devices on the system. In this manner, a unique Universal Resource Locator (URL) can be defined for each device on the system. Typically, in an Ethernet environment, each network controller will have

a unique serial number associated therewith, there never being two identical serial numbers in any network controller or network card for the Ethernet environment.

[0065] In the transaction packet, there are provided a plurality of smaller packets that are referred to as "ID packets" that are generated in the application level. This basically comprises the data field 402. The transaction packet is formulated with a plurality of these ID packets and data that are generated at the transaction node and modified at other nodes. This transaction packet, once formed, is transmitted to the network level in such a manner that the appropriate header will be placed thereon to send it to the appropriate location. Therefore, the software or process running at the particular transmitting node on the network will have some type of overhead associated therewith that defines the address of the source node on the network and also the address of the destination node. Therefore, when data is received by any one of the nodes, it can recognize the defined field for the destination address as being its address. Further, it can utilize the information in the source address field, which is at a particular location in the data packet, to determine where the data came from.

[0066] Referring specifically to FIGURE 4B, there is illustrated a diagrammatic view of an ID packet 430. The ID packet 430, in the present disclosure, is comprised of a plurality of IDs, a core ID 432, a device ID 434 and an item ID 436. The core ID 432 is that associated with a particular entity on the network such as a corporation. For example, if a corporation had a profile set up, it would be assigned this particular core ID when initiated. The device ID 434 is the unique ID of the device on the network. The core ID could be the corporation, and the device ID could be the computer or program that is assigning item IDs. For example, if company ABC had an assigning device, a computer EFG, the computer EFG would be the creator of the ID packet. If device EFG wanted to assign a vendor ID to a particular vendor - the item, then vendor ID would be set to HIJ. The value for the data packet would then be ABC/EFG/HIJ. Note that the ID is actually not letters, but a combination of codes and time stamps.

[0067] Each of the core ID 432, device ID 434 and item ID 436 are comprised of two blocks, a group block 438 and an individual block 440. The group block and the individual block 440 are comprised of a prefix 442, a time stamp 446 and a sequence number 448. The prefix is a sequence of predetermined prefixes that define various items associated with a particular group or individual. For example, it could be that the setup of the profile define this individual as a vendor that had an account which was a core ID and other various prefix values. As such, many different companies or organizations could have the same prefix. However, once the prefix is defined, then the time that it is created is set in the time stamp 446 and then a sequence number is associated therewith in the field 448. Therefore, since only one entity will ever assign the time stamp and sequence values, the entire block, 438 will comprise a unique value or number or ID for that particular group. For example, if company A set up a profile, it would be assigned a unique number that would always identify that particular company and this would never change. As far as the individual block 440, this is a block that further defines the core ID. For example, there may be five or six different divisions within a corporation such that this can be a subclassification. The notable aspect for this particular core ID 432 is that it comprises a unique ID in the system and will define certain aspects of the overall ID packet 430, as well as the device ID 432, 434 and item ID 436. When all three of these core ID 432, device ID 434 and item ID 436 are combined, this defines a unique ID packet 430 that is associated with various information such as transactions, messages, pointers, etc. These are set up originally in the universal ID server 132 in a profile origination step (not described) wherein a particular operation can be associated with the ID packet 430. This would essentially constitute a relational database somewhere in the system. Therefore, as will be described in more detail hereinbelow, when this ID packet 430 is assembled into the transaction packet, it is only necessary for any node to examine each of the ID packets and determine if any of the ID packets define operations to be performed by that particular ID packet. For example, if the ID packet represented a transaction such as a conversion, then the conversion server 150 in, for example, system 104, would recognize the particular ID packet indicating a conversion operation and also it might require information as to the destination node which is typically information contained in an ID packet, among other







a column 504. The column 502 is a date stamp on a given row, such that the particular row when accessed can be date stamped as to the time of access. A row ID that is proprietary is also associated with the accessed row. Therefore, whenever a row is accessed, it is date stamped and assigned a row ID. In this manner, even if the data is reorganized through a database packing operation or the such, the data can still be found. As such, a unique identification number for a given row can be generated with the proprietary row ID or the proprietary RID and the date stamp, such that a large number of proprietary numbers can be realized.

[0071] When the databases are generated and put in the appropriate formats, it is desirable to transfer data that is stored for the purpose of a transaction to actually facilitate or execute the transaction. This utilizes a unique "Extent" for that transaction, which Extent is defined by an arrow 506 that converts the data in the appropriate manner to a proprietary transaction packet 508. The Extent 506, as will be described hereinbelow, is operable to determine how to process data, extract it from the various tables, even creating intermediate tables, and then assemble the correct ID packets with the appropriate data in a transaction packet and transfer this transaction packet to the network. Since the transaction is a profiled transaction for the whole network, the entire decision of how to route the data and ID packets to the destination and the manner in which the data is handled or delivered to the destination is not necessarily determined in the Extent at the H1 transaction node. Rather, only the information necessary to "launch" the transaction from the transaction node H1 is required and which ID packets are to be included. Once it is launched to network, this unique transaction packet travels through the network and is processed in accordance with the unique ID packets embedded in therein.

[0072] Referring now to FIGURE 6, there is illustrated a diagrammatic view of two transaction nodes 602, labeled H1, and 604, labeled H2, in a system that are both associated with individual routers 606, labeled R1, and router 608, labeled R2. Router 606(R1) is interfaced with the transaction node 602 through a local network 610, which also has associated therewith two conversion servers 612 and 616, labeled C1 and C2,

respectively. The router 606(R1) is interfaced with router 608(R2) *via* a network 618. Router 608(R2) is interfaced with transaction node 604 through a local network 620, network 620 also interfaced with a conversion server 622 labeled C3.

[0073] In operation, there will be a channel defined for any given transaction. This channel will define the path that is necessary to traverse an order to “hit” all the necessary processing nodes in order to effect the transaction in the appropriate manner and in an appropriate format that will be compatible with transaction node 604 when it arrives thereat. Similarly, if the transaction node 604 desires to utilize the same transaction back to node H1, it would merely use the same channel but in the reverse direction. Similarly, another transaction could be defined from the transaction node 604 to 604 directed toward transaction node 602, requiring an additional channel. Of course, each of these would also require a unique feed ID packet that would define the various software that generated the various channels, ID packets and the data packets, as described hereinabove.

[0074] Referring now to FIGURES 7A and 7B, are illustrated graphical depictions of two channels. In FIGURE 7A, there is illustrated a channel from H1 to H2 labeled “0011.” This channel requires the data to be generated at H1 and transferred to R1. At R1, a conversion operation is determined to be required and the data is merely sent to converter C1 (after possible caching at the router.) At conversion server C1, the conversion is performed and then it is reassembled and passed back to R1. At R1, it is determined that the data packet has arrived from C1, and the next step is to send it to converter C2. Converter C2 then performs the appropriate conversion operation, based upon the feed ID packet and the other unique ID packets in the transaction packet, and then transfers the transaction packet back to R1. At R1, it is determined that this transaction packet must be sent to another router, which is router R2. When sent to router R2, the routing information could be global or it could be network specific, *i.e.*, the channels might be specific only to the systems associated with the appropriate router. In a situation like this, an intermediate “joiner ID” is generated that defines a particular relationship. This is an intermediate ID that is created for the purpose of this particular transaction. This joiner ID then is

generated and the information sent to the router R2 which indicates that router R2 is to transmit the transaction packet to H2. It is known in this particular channel and transaction that the transaction packet is already appropriately conditioned for receipt by H2 and H2 will receive the transaction packet, and know what type of transaction is to be performed at H2, *i.e.*, it is aware of the unique ID packets and their meaning, such as the feed ID, packet how to process information once received, etc. It therefore understands the parameters within which the transaction is to be effected.

[0075] In FIGURE 7B, there is illustrated another channel, channel "0022" for performing another transaction from H2 over to H1. This channel requires that the transaction packet be sent from H2 over to R2 and then from R2 over to C3 for conversion. After conversion, the transaction packet is sent from C3 over to R2 and then from R2 over to R1 with a joiner ID, similar to that of FIGURE 7A. At R1, the data is transferred directly to H1. If the transaction for this particular channel is to be transmitted back to H2 along the same channel, the reverse path would be utilized.

[0076] Referring now to FIGURE 8, there is illustrated a flow chart for initiating a transaction. When the transaction is initiated, it is initiated at a block 802 and then a transaction table is created. This transaction table will have data associated therewith with rows of data therein in a predetermined format that is associated with the native database of the transaction node. This transaction table will then have each row therein stamped with a proprietary date and a proprietary RID, as indicated by the function block 804. Thereafter, the transaction flow will be analyzed, in a function block 806, to determine how the data is to be arranged and transferred. This transaction is then scheduled for transmission, in a function block 808. This is facilitated with a process wherein various calls are created for each block of data in the database, as indicated by a function block 810 and then a run ID is created in a function block 812. After the schedule has been generated and queued, the program then flows to an End block 814.



decision block 914. If it is not to be divided, the program will flow from the decision block 910 to the input of decision block 914.

[0079] Decision block 914 determines if more data is to be extracted from the local database of the transaction node initiating the transaction and, if so, the program flows back to the input of function block 902 to pull more data. Once the data associated with the transaction has been extracted, the program will flow to a block 920 to return the operation.

[0080] Referring now to FIGURE 10, there is illustrated a diagrammatic view of a sample transaction table. The transaction table is basically comprised of the message number, the transaction ID, the joiner ID (if necessary), the row ID and date with proprietary identification system and the block ID. Also, a RUN ID can be assigned to each block as it is being processed. The row ID in a column 1002 and the date in a column 1004 is different from the database defining row ID in that they are always associated with the row. The row ID in the database is defined as function of the database and can actually change through various rearranging of the database at the transaction node.

[0081] Referring now to FIGURE 11, there is illustrated a flow chart depicting the operation of actually exporting the data from the transaction table. This is initiated at a block 1100 and then flows to a function block 1102 to pull the first block in accordance with the Extent that is running. It should be understood that all of the flow charts from the start of the transaction to the end of a transaction are associated with a predetermined transaction Extent. This Extent, as will be described hereinbelow, is a sequence of instructions or codes that are downloaded to the particular node to allow the node to conduct its portion of the transaction in the predetermined manner defined by the transaction profile that is distributed throughout the system. Not all of the necessary transaction information is contained here but, rather, only the information or the process steps necessary to create and transmit the transaction packet out of the system in the correct manner.

**[0082]** Once the data is pulled in accordance with the Extent running on the transaction node, the program will flow from the function block 1102 to a decision block 1104 to determine if a caching operation is to be performed. If not, the program will flow to a function block 1106 to process the block as pulled. If caching is required, the program will flow to a decision block 1108 to determine if the caching is done, before transmitting the blocks and, when complete, the program will flow to a decision block 1108, along with the output of the function block 1106. The decision block 1108 determines whether an encryption operation is to be performed. If the data is to be encrypted prior to transmitting over the network, the program will flow to a function block 1110. If not, both function block 1110 and decision block 1108 will flow to the input of a function block 1112 to assemble the data packet. It is noted that the encryption operation is something that is optional and does require the overhead in each recipient node to decrypt the data. This function will not be described with respect to the remainder of the data flow.

**[0083]** Once at the function block 1112, the transaction packet is assembled. The program then flows to function block 1114 to determine if the transaction packet is completely assembled and, once complete, the program will flow to a transmit block 1116.

**[0084]** Referring now to FIGURE 12, there is illustrated a flow chart for the transaction packet assembly operation, as initiated at a block 1202. The program flows to the function block 1204 to determine the size of the data packet, whether it is a small group of ID packets in the transaction packet or plural ID packets in the transaction packet. Once the size of the transaction packet has been determined, the program flows to a function block 1206 to determine the router to which information is to be transmitted. It is noted that more than one router could be on a network. The router is determined, of course, as a function of the particular Extent that is running, this being the path to which the packet will be routed. Once determined, the program will flow to a function block 1208 to insert the feed ID and the channel ID. It is noted that the feed ID and the channel ID are inherently

a part of the Extent, this having been determined at the generation of the feed Extent which was generated during the profiling operation, as will be described hereinbelow. The program then flows to function block 1210 to attach the Run ID thereto and then to a Return Block 1212.

**[0085]** Referring now to FIGURE 13, there is illustrated a diagrammatic view of a transaction or process that is originated at an origin node 1302 for transmission to the destination node 1304 on a single outgoing channel. As noted hereinabove, the outgoing channel defines the route and the transaction. The origin node at 1302 utilizes a local Extent, indicated by box 1306, to generate the transaction. In this transaction, there are a number of IDs that are generated. One is a "RUN ID," one is a "FEED ID," and the third is a "CHAN ID." Although there may also be other ID packets that are generated, these three packets can basically define an entire transaction or process.

**[0086]** The origin node 1302, which can comprise the host node or the such, generates the transaction packet comprised of at least the RUN ID, the FEED ID and a CHANNEL ID and forwards it to a first process node 1306 which processes the received transaction packet in accordance with the above noted processes which then requires the transaction packet to be modified and transferred to a second process node 1308 for further processing, which then forwards this to a third processing node 1310 and then to a fourth processing node 1312 before final routing to the destination node 1304. The destination node 1304, as described hereinabove, can be the system router. Additionally, the router could be one of the processing nodes 1306-1312. This process will use a single outgoing channel for transferring a transaction packet from the origin node 1302 over to the destination node 1304. At the destination node 1304, the information could be transferred out of the channel to another channel, as will be described hereinbelow. Overall, this processing channel is defined graphically as a block 1314. This graphical representation indicates that a transaction packet is generated and the process through various nodes in accordance with distributed processing described hereinabove to route the transaction packet along various processing nodes to the destination node 1304 for handling thereat.

[0087] Referring now to FIGURE 14, there is illustrated a diagrammatic view of two channels adjacent to each other. In this embodiment, there is illustrated an origin node 1402 which is operable to generate a transaction packet, as described hereinabove, through two processing nodes 1404 and 1406 to a router 1408, labeled R1. This router R1 is substantially the same as the destination node 1304 in the single outgoing channel noted with respect to FIGURE 13. This combination of the origin node 1402, the two processing nodes 1404 and 1406 and the router 1408 comprise an outgoing channel. A second channel is associated with a destination node 1410. The overall transaction or process is operable to generate the transaction at the origin node 1404 and route it finally to the destination node 1410 for completion of the transaction. However, once the router 1408 has received the transaction packet, it then passes it over to a router 1412 labeled R2, which constitutes an incoming channel for the destination node 1410. The router 1412 receives the packet from router 1408 and passes it through two processing nodes 1414 and 1416 to the destination node 1410. As noted hereinabove, the two systems, the one associated with router 1408 and the one associated with router 1412 could handle the transaction packet and the ID packets associated therewith in a similar manner, *i.e.*, that is, they could utilize the same packet IDs. However, for security purposes, the origin node 1402 and the destination node 1410 utilize a different set of ID packets referred to as joiner ID packets to transfer information therebetween. As such, within the outgoing channel associated with router 1408 and origin node 1402, there would be a defined set of system assign IDs that would be proprietary to the origin node 1402. It may be that the actual identification of these IDs is something that the origin node 1402 would not want to share with the destination node 1410. Therefore, the origin node 1402 and the destination node 1410 negotiate a relational database that associates an arbitrary joiner ID with various IDs at the origin node 1402 such that the IDs have no meaning in any system other than for the business relationship between the outgoing channel and the incoming channel for the origin node 1402 and destination node 1410, respectively. These joiner IDs are illustrated in tables of FIGURE 14A. You can see that router R1 has a table associated therewith wherein the joiner ID "0128" is associated with an ID packet "XXXX." Whenever this



joiner ID is received by router R2, a table for router R2 is examined to determine that this joiner ID "0128" is associated with an ID packet "ZZZZ" therein. For example, it may be that there is a unique ID associated with origin node 1402 that defines it in an overall system. However, it may be that destination node 1410 defines the origin node 1402 in a different manner, *i.e.*, as "ZZZZ." Rather than redefine the joiner ID as "XXXX" in its system, it merely needs to have a joiner ID that defines the relationship between the two systems. Therefore, whenever the joiner ID "0128" is received as an ID packet, the router R2 will convert this joiner ID to the ID packet "ZZZZ" such that it now recognizes that ID packet as the vendor number of the origin node 1402 within its system. Other than within the system associated with destination node 1410, this has no meaning.

[0088] With respect to the joiner IDs, the joiner ID can be associated with the transaction packet in any position along the processing path. Typically, the joiner ID is assigned at the origin node 1404 when running the Extent associated therewith, *i.e.*, it is initially defined when the feed and the channel are assigned. However, it could actually be assigned at the router 1408.

[0089] Referring now to FIGURE 15 there are illustrated three separate processing blocks 1502, 1504 and 1506, similar to the processing block 1314. Each of these processing blocks 1502, 1504 and 1506 represent a single channel and a processing system. For example, processing node 1502 could represent a single company and its associated router, conversion server, ID server, archival server and host node. When performing a transaction to transfer to another system, the transaction packet is generated within the processing node 1502, processed therethrough in accordance with the distributed processing system as described hereinabove and then output from the processing block 1502 over to a second channel 1508 for routing to the processing block 1504. The processing block 1504 represents a third channel and an independent and self-contained processing block. For example, the processing node 1504 may be an intermediate processing node that allows independent processing of a transaction or processing event for transfer to the processing block 1506. This could be, for example, a satellite system that constitutes an intermediate

processing step. Once the transaction has been processed through the third channel, this is then transferred to a fourth channel 1510 for transfer to the block 1506, which comprises a fifth channel. Each of these channels and each of these processing blocks comprise separate distinct processing operations which all operate on the same transaction packet (although the transaction packet may be modified somewhat). Initially, the processing block 1502 originates at an originating node therein the transaction. This transaction has a channel and feed associated therewith, which channel comprised all of the channels from the origin to the destination at processing block 1506.

[0090] Referring now to FIGURE 16, there is illustrated a diagrammatic view of how the channel IDs and the feed IDs change as the transaction packet is processed through various processing nodes. As described hereinabove, a channel is defined as the route that a transaction path is to take through the various processing nodes. Since the processing is distributed, the transaction packet must be routed to each node in order that the appropriate processing be carried out on that transaction packet. Since the processing is predefined with respect to the channel ID, very little information needs to be disposed within the transaction packet in order to effect the processing. This transaction packet and the packet IDs associated therewith in the form of the feed ID, the channel ID, etc., define the portion of the processing that is to be carried out at each processing node, *i.e.*, these constituting process pointers at each processing node. With respect to the channel ID, this basically remains the same in the transaction packet as the transaction packet traverses a group of processing nodes. However, the feed ID will change. The feed ID basically constitutes an instruction that is generated at one processing node for transfer to the second processing node that defines the processes that are to be carried out. In general, this feed ID is a "tracer" that follows the process to flow from node to node. As such, when one node receives a transaction ID from another processing node, it recognizes that the process is that associated with the channel ID, but it also recognizes where in the process the transaction packet is. For example, a router may handle a transaction packet a number of times in order to effect transfer to one or more conversion servers, effect transfer to an ID server, etc. With the use of the feed ID, the router now has knowledge of what process is

to be carried out in the overall transaction process when it receives the transaction packet from a given processing node. Additionally, another aspect that the feed ID provides is the tracing function wherein a failure at any point along the process path can now be tracked to the previous process that was carried out.

[0091] With specific respect to FIGURE 16, there are provided a plurality of processing nodes 1602 labeled N1, N2, . . . , NK. Each of the processing nodes 1602, as described hereinabove, carry out a portion of the overall transaction process which was predistributed to the processing node. Each of the processing nodes 1602 carries out a plurality of processes, labeled P1, P2 and P3 for exemplary purposes. It should be understood that any number of processes could exist at a particular processing node 1602 that could be associated with a given channel ID or multiple channel IDs for many other transactions apart from the current transaction. It is noted that each processing node can handle many different processes and transactions. Once a transaction ID packet is configured, each processing node will receive that transaction packet, examine the transaction packet and determine exactly which process must be performed on that transaction packet, all of the effected with only a few ID packets of a fixed length.

[0092] When the transaction is initiated, it is initiated at the origin node, illustrated as a node 1604 for generation of a feed ID and a channel ID, labeled FEED1 and CHID1. This indicates at the origin node 1604 that this transaction packet is to be transferred to processing node N1. When processing node N1 receives the transaction packet, it recognizes that the process to be carried out is defined by the feed ID and it has associated therewith a FEED1 block 1606 that defines the process that is to be carried out. This block 1606 then can select between the available processes P1-P3 for application to the transaction packet. Once a transaction packet has been processed in accordance with the selected one of the processes (it may possibly require more than one process for the processing), then the feed number is changed to the next feed ID, FEED2, and then the transaction packet is transferred with the same channel ID, CHID1, to the next processing node, node N2. At this node, the processing node recognizes that this is the FEED2 feed



Typically, the ID server, the host node, the conversion server, and the network mesh are all typically associated and “owned” by a particular company.

[0094] Referring now to FIGURE 17, there is illustrated a diagrammatic view of how the feed is incremented. This is initiated at a start block 1702 and then proceeds to various feed blocks for the feeds FEED1, FEED2, . . . , FEEDK. The process must go through each of the feed blocks and, at each of the feed blocks, carry out the associated process. Therefore, the transaction packet in effect not only carries a channel ID that can be utilized at a particular processing node to determine what transaction is being processed but also receive intermediate instructions to indicate what processes in the transaction are to be carried out. As noted hereinabove, it may be that the router is involved in the actual transaction a number of times. Although a plurality of processes are predetermined as being associated with the given transaction, the processes that are applied to the transaction packet are determined as a function of where in the process the transaction is. The feed IDs indicate the position in the transaction for the purposes of determining which predetermined transaction processes are to be applied to the transaction packet when received at a particular processing node. Additionally, the feed IDs also provide for some failure analysis in the event that a failure occurs. For example, in FIGURE 15, one could examine any transaction or process from the origin to the final destination at any place in the process and determine where in the process it was.

[0095] Referring now to FIGURE 18, there is illustrated a flow chart depicting the operation of running the process at a given process node. The program is initiated at a block 1802 and then proceeds to a function block 1804 to read the feed ID received in the transaction packet. The program then flows to a function block at 1806 to run the process or processes associated with that feed ID and then to a decision block 1808 to determine if all the processes have been run. If not, the program continues running processes in the block 1806 and, when complete, the program flows to a function block 1810 to increment to the next feed number and then transmit the transaction packet to the next processing node, as indicated by a return block 1812.

[0096] Referring now to FIGURE 19, there is illustrated a diagrammatic view of a plurality of channels which indicate processing from an origin to a destination in each channel and then handing off to a second channel or second system. These are defined as channels CH1, CH2 and CH3. In channel CH1, there is provided an origin node 1902 and a destination node 1904 with two processing nodes 1906 associated therewith. In the second channel, CH2, there is provided an origin node 1908 and a destination node 1910 with three intermediate processing nodes 1912. In the third channel, CH3, there is provided an origin node 1914 and a destination node 1916 and three processing nodes 1918. The transaction is initiated at the origin node 1902 for final transmission to the destination node 1916. However, between the destination nodes 1904 and 1908, there is provided a line of demarcation 1920, with a similar line of demarcation 1922 disposed between destination node D2 and origin node 1914. The destination node 1904 could be a router and the origin node 1908 could be a router in channel CH2. The line of demarcation 1920 indicates that the first channel, CH1, basically "hands off" the transaction to the second channel CH2 which processes the transaction in accordance with a predetermined process set forth therein in a distributed manner across the various processing nodes for handing it off to the third channel, CH3. Each of the line of demarcations 1920 and 1922 define distinct boundaries such that the transaction packet can be considered independently handled for each of the channels. For example, it may be that in order to transfer from CH1 to CH2, a joiner ID is provided. When handing off from destination 1910 to origin 1914 across line of demarcation 1922, a second joiner ID' may be required.

[0097] Referring now to FIGURE 20, there is illustrated a diagrammatic view of one of the systems of 102-108 wherein a non-system node 2002 is interfaced with the system 104 through a network 2006, which interfaces with the router 136. The non-system node 2002, since it is not part of the overall system 104, is not identified in the system per se without some processing in the system 104. In general, the non-system node 2002 first must be identified and the transaction associated with its access to the router 136 identified. Once

this identification is made, then the necessary transaction packet is assembled and the transaction conducted in accordance with the process described hereinabove. For example, the non-system node 2002 will initiate a transaction merely by contacting the router 136. This could merely be the transmission of a request to a specified URL of the router 136 on the network 2006. The router 136, upon recognizing the URL of the non-system node 2002, *i.e.*, the source URL, would recognize that a transaction is being initiated. The router would then create a transaction packet and route it to the conversion server 150. The conversion server 150 would then convert information received from the non-system node 2002 over to a format compatible with a transaction to be conducted with, for example, transaction node 140 on the network mesh 138 in the system 104.

[0098] As an example of a transaction, consider that the non-system node 2002 wanted to send an order via e-mail to transaction node 140. To facilitate this, non-system node 2002 would fill out a form in a predetermined order with information disposed in predetermined fields. This e-mail would then be routed to the router 136. The router 136 would recognize the source of the e-mail and the fact that it was an e-mail. By recognizing both the source of the e-mail and the fact that it is e-mail, the router 136 would now recognize a transaction. It would create a form ID for the non-system node 2002, which would define the type of form that is to be routed to the conversion server 150, and various other IDs that are associated with the transaction. This form and the form ID, in addition to other identification information in the form of ID packets, would be sent to the conversion server 150. The conversion server 150 would then extract the information from the form in accordance with the form ID pointer, and convert this to information associated with the transaction. This would then be transferred to transaction node 140.

[0099] Referring now to FIGURE 21, there is illustrated a flow chart depicting the operation of the router 136 when receiving information from within the system and from outside of the system. The operation of the router 136 is operable to receive data in the form of packetised data from the non-system node 2002. This is indicated at decision block 2102. The program then proceeds to decision block 2104 to determine whether this

is a system packet. If so, then this indicates that this is a system node and the program will proceed to a function block 2106 to process the received transaction packet in a normal mode. If it is not a system packet or transaction packet, the program would flow to a function block 2108 to convert the packet to a system packet and then to the function block 2106.

**[0100]** Referring now to FIGURE 22, there is illustrated a block diagram of a simplified embodiment of FIGURE 20. In this embodiment, there is illustrated a situation wherein the non-system transaction node 2002 can do nothing more than access the router 136 and transfer information thereto. As such, the router 136 must have some type of ID process, indicated by block 2202, by which to recognize the non-system node 2002 and associate the transaction packet therewith, which involves the use of a form ID, as described hereinabove. Once the transaction packet is created by the router 136, then the transaction packet is routed to the conversion server 150 and a conversion process, as indicated by block 2204, is run and the information received from the non-system node 2002 converted to the appropriate format to complete the transaction.

[0101] Referring now to FIGURE 23, there is illustrated an alternate embodiment of the embodiment of FIGURE 22, wherein the non-system transaction node 2002 has software associated therewith that allows it to form the transaction packet. The non-system node 2002 has an ID process block 2302 associated therewith that allows the non-system node 2002 to create a transaction packet. The non-system node 2002 has a definite ID on the system which has been defined in the original setup wherein the ID process in block 2302 was created and “pushed” out to the non-system node 2002. Whenever a transaction is to be implemented, the ID process is run and a transaction packet assembled. This transaction packet is then forwarded to the router 136, in accordance with information in the transaction packet. This is due to the fact that the transaction packet created by the ID process 2302 has a channel ID and the such contained therein.



[0102] Once the router 136 receives the transaction packet, it recognizes this transaction packet as one that exists on the system and routes it in accordance with a routing process in a process block 2304. Thereafter, this transaction packet is modified, if necessary, and routed to the conversion server 150 for processing thereby. The routing to the conversion server 150 is in accordance with the channel definition set forth in the ID process 2302. Thereafter, the information is processed as described hereinabove with respect to FIGURE 22.

## **ID PACKET**

[0103] Referring now to FIGURE 24, there is illustrated a more detailed diagrammatic view of the ID packet that constitutes the proprietary portion of a transaction packet that is transferred over the network, it being noted that this ID packet is typically embedded within a data transmission between the network with all of the commensurate overhead associated with such a transfer. As was described hereinabove, this ID packet represents the smallest fixed length portion of a transaction packet.

[0104] The ID packet is divided into three sections, a core ID section 2402, a device ID section 2404 and an item ID section 2406. Each of the sections 2402-2406 are divided into two sections, a "Group" ID and a "Individual" ID section. A detail is illustrated of the core section 2402. Each of the Group and Individual sections are comprised of three sections, a preamble section 2408, a time stamp section 2410 and a sequence section 2412. As described hereinabove, the preamble section 2408 comprises a classification section that is comprised of a plurality of "classifiers." The time stamp section 2410 and the sequence section 2412 provide a unique value that, when associated with a classifier section 2408, provides a unique group value for the core section 2402. The Individual section is also organized as such. In the preamble section 2408 of the Group section, it can be seen that there are a number of classifiers associated therewith. Of these, one classifier will always be the classifier "G." There can be multiple other classifiers, it being understood that the number of classifiers is finite. As will be described hereinbelow, each of these classifiers

is comprised of a single alpha character, there being twenty-six alpha characters, each of which can be represented by an ASCII value which is a finite length value. Of course, this limits the number of values to twenty-six for each classifier field. There could be any type of value system utilized, it only being necessary that the field be a fixed length. For example, if the field were defined as a digital word having a four bit length, this would provide  $2^4$  values. With respect to the preamble 2408 on the Individual section, this also has a finite number of classifier fields, one of which will be the classifier "T" designating this as an Individual ID.

[0105] The core ID 2402, device ID 2404 and item ID 2406 are illustrated in Table 1 as follows:

**TABLE 1**

<b>CORE (WHO)</b>	<b>DEVICE (WHERE)</b>	<b>ITEM (WHAT)</b>
Corporation or Entity	Assignee of the Packet, e.g., computer, phone, etc.	Object, e.g., article, net address, real estate property, etc.

[0106] The core ID 2402 is directed toward the basic owner of the ID packet. This, for example, could be a corporation, such as Corporation ABC. The device ID is associated with the device that assigned the values in the packet. For example, this could actually be the ID of the computer, the phone, etc. that actually was responsible for assigning the packet. The item ID is the subject of the data packet or the object, *i.e.*, an article of commerce, a network address, a real estate property or the such. This is referred to as the "Who, Where, What" aspect of the ID packet. For example, Corporation ABC is originally defined as the owner of the ID packet. A unique core ID is initially associated with the ABC corporation wherein a defined classification preamble 2408 is associated therewith and then a unique time stamp and sequence number. This classifying preamble 2408 may actually be identical to the classification associated with other corporations in the system. However, once the time stamp and sequence number are associated with the preamble

2408, this core ID becomes unique as to that corporation or entity against others. When an object or item is being incorporated into an ID packet, *i.e.*, an ID packet is being created to uniquely define that item in the system, there is some device on the system that actually creates this ID packet. For example, it might be that a catheter is being uniquely defined in a company. There will be possibly a computer terminal on which the information is entered. This computer terminal has an ID in the system and it is this ID that comprises the device ID. Therefore, once the ID packet is created, the entity (corporation) then owns the ID packet. The object, *i.e.*, the catheter, is classified and is also known which device assigned the ID packet or created the ID packet.

[0107] Referring now to FIGURE 25, there is illustrated a more detailed diagram of the preamble 2408. The preamble 2408, as described hereinabove, is comprised of a plurality of fields. These are referred to in FIGURE 25 as “F1, F2, F3, F4, F5, . . .” There are a fixed number of fields for the preamble 2408 which, in the present disclosure, are fixed for each Group ID and Individual ID for each of the core, device and item IDs. However, it could be that the fields differ between preambles, the only requirement being that they do not differ between ID packets. A typical five field preamble section of an ID is illustrated in Table 2 as it exists in the database, understanding that more fields may be incorporated.

## TABLE 2

F1	F2	F3	F4	F5	TS/SEQ	CONTENT
A	B	Z	C	W	XXXX	—
C	T	Q	I	C	XXXX	—
F	L	A	K	L	XXXX	—
G	M	B	R	S	XXXX	—

**[0108]** With reference to Table 2, it is described hereinabove that each field has an alpha character associated therewith. This alpha character has a predefined relationship for the

classifier. For example, if a field were associated with the type of ID, there could be two values, one associated with a permanent ID and one associated with a joiner ID. This would therefore be a field having only two values. It could be that this utilized the alpha characters "P" and "J." However, it could use any alpha character (number, character, symbol, etc.), it being recognized that the value or relationship (meaning) of the characters is unimportant; rather, it is the relationship of that packet disposed in other locations in the system that is important. In TABLE 2, it can be seen that the database associated with a particular ID has associated therewith the fields in the preamble, the time stamp/sequence field (TS/SEQ) section in addition to a content column. The content column defines what this preamble is associated with. For example, if this were the Group ID in the core ID 2402, then this could refer to, for example, a content of "chemical corporations." If this were Corporation ABC, then the Individual ID would have a preamble field that might be common with other individual corporations but the TS/SEQ section would be unique only to that corporation and the content associated with that particular corporation would have the term "Corporation ABC" in the content column. It may be that there are ten corporations that have identical preambles but different TS/SEQ values and, therefore, the core ID 2402 would be unique to that corporation. Each of the Group ID and Individual IDs for the core, device and item IDs in the ID packet would be configured similarly.

**[0109]** As will be described hereinbelow, although each of the fields in the preamble 2408 is defined as having only 26 values due to the choice of an alpha character as the classifier, one of the fields can be combined with the TS/SEQ value to provide a larger value associated therewith. Since the TS/SEQ value can comprise a unique and very large number, it does not constitute a classifier as such. By combining the twenty-six alpha numeric values each with the TS/SEQ value, the number of classifiers for that particular field becomes very large. For example, if one wanted to define a field in the preamble for the item ID 2406 as the field that defines the item, more than twenty-six item classifiers can now be provided. As a simple example, it could be that there are a plurality of catheter types in a company such as a pulmonary catheter, a cardiac catheter, etc. If there are more than twenty-six of these types of catheters, there would be required more than twenty-six

classifier values. By combining an alpha character with the time stamp, the number of available classifiers can be increased in value.

[0110] Referring now to FIGURE 26, there is illustrated a diagrammatic view of the classification scheme. There are illustrated four fields that are being classified in a preamble, it being understood that more or less fields could be defined for the preamble structure, with only three values illustrated for each field. However, each of these values can be conditional upon the previous path, as will be described hereinbelow. In the field F1, there are illustrated three classifier values, A, B, C. The classifier of interest in field F1 is "A." There are illustrated three paths from this classifier, since field F2 is only associated with three classifiers, these being again, A, B, and C. It should be understood that the classifications being associated with the classifier A is not necessarily the same classifier associated with the classifier A in field F1. Also, the classifier B in field 1 may also point to three separate classifiers A, B and C in field F2. However, it should be understood that the classifier A in field F2 that the classifier B in field F1 could point to may not be the same as classifier A in field F2 pointed to by the classifier A in field F1. The classifier in any one of the fields below field F1 has a value that may be conditioned upon the classifier in the previous field from which it derives. It can be seen that each of the classifiers in field F2 will point to one or more classifiers in the next field F3, there being illustrated three, A, B and C. Further, field F4 further expands this will three classifiers, A, B and C for each of the classifiers in field F3. Again, although there are illustrated as multiple classifiers A in field F3, they are not identical in value or classification function but, rather, they are unique to the associated path.

[0111] With reference to FIGURE 27, there is illustrated a single path through a given preamble of a field width of four. In the Group ID, for example, the preamble may be classified as "A" in field F1 and it may point to classifier "B" in field F2. Although the path could go to classifiers "A" or "C" only one path is selected. At field F2, classifier B points to classifier "A" in field F3 and classifier "A" in field F3 points to classifier "B" in field F4. Therefore, once it has been determined that field F1 has classifier A, then the next

determination must be which of the classifiers in field F2 associated with classifier A in field F1 will be selected. It is this association of classifiers in a lower field with those in an upper field that defines the classification scheme. Again, it could be that classifier "B" in field F1 could point to a classifier "B" in field F2 that is different than that associated with classifier "A" in field F1. However, it could be that some fields have identical classifiers for each of the above fields. For example, in the Group ID, the last field will always be "G" defining the Group ID as such (not a conditional classifier.) The individual ID will always have a "I" in the last field thereof defining it as such. Therefore, there need not be any association between fields though there can be an association. With respect to the Individual ID, this follows the same path as the Group ID with the exception that it is defined as having values of "D," "E," and "F."

[0112] The ID that is generated will be stored in a table in the database of the ID server with alpha titles that can be searched, in association with the code associated therewith. A typical table in the database is illustrated in Table 3. In Table 3, the field F1 is associated with an ID that is either a permanent ID or joiner ID. This is referred to as P/J in one column, this is defined as a permanent or joiner field with the code associated with the permanent field being a "P" and the code associated with the joiner field with the joiner value being a "J." The second field F2 is associated with different types of devices are Individual IDs or Group IDs, defined, in this embodiment as a profile type, a network type or a system type. Therefore, the one column will define the type as being profile, network or system and the code associated with the profile type will be "F," the code associated with a profile type would be "P," with a network type would be "N" and with a system type would be "S." Field F3 is associated with an item which could be a type of computer such as an Apple computer, an item such as a catheter, a URL for a network address or the name of a system such as AVC or with a system referred to as a PLL, this basically being an acronym for some type of system in the industry, as an arbitrary example. In this example, the code is the combination of an alpha character plus the time stamp for that row, to provide a large number of values therefor. In field F4, this is the category of the ID which, in this example can either be a core ID or a vendor ID. If it is a core ID, it will have a code

of "C" and if it is a vendor ID, it will have a code of "V." There will also be a time stamp associated with each row. It can be seen that there are two IDs having identical values in all of these fields with the exception that field F3 is associated with different catheters. As such, the code value would be distinguishable between the two because the code P+TS is associated with a different time stamp. This is what makes these two IDs distinct, even though they are associated with the same item, they are both vendor IDs, they are both permanent IDs and they are both profile IDs. By utilizing the time stamp in association with a alpha character, a much larger number of items can be defined for this particular field.

[0113] Referring now to FIGURE 28, there is illustrated a diagrammatic view of the method in which the data packet is created and the database populated with the data packet. Initially, a profile screen 2802 is provided which provides a plurality of user modifiable fields 2804 that allow the user to insert information. Each of these fields is utilized for the classification operation. Sometimes, this is an interactive system wherein inserting information into one field will result in another type of field being made available. For example, if somebody were classifying a data packet as being associated with a network, it might be that the URL of the network were provided as a possible input for another classifier, whereas that particular classifier, the URL, might not be appropriate for a previous classifier.

[0114] Once the user has inserted all of the necessary information, then the flow would move to a block 2806 wherein the information that is input by the user would be classified into the preamble of the appropriate ID in the data packet. This, as described hereinabove, would be required in order to classify all of the IDs in the ID packet. For example, when filling the profile, a corporate name would be specified which automatically would pull up the core ID for that corporation. Of course, the device that is being utilized to fill in the profile would already be known and would constitute the device ID. The remaining portion of the profile 2802 would be utilized for the purpose of providing the item profile. The classifier would assemble all of this information and then flow to a block 2808 wherein the data packet is populated and the database is populated, as indicated by block 2810. This

population of the database would provide information associated with the ID packet, as set forth in Table 3, such that all of the information necessary to identify a ID packet is contained therein. Table 3 is as follows:

**TABLE 3**

F1		F2		F3		F4		F5
P/J	Code	TYPE	Code	ITEM	Code	CATEG	Code	
Perm	P	Profile	P	Apple	D+TS	CORE	C	—
Perm	P	Profile	P	Cath	P+TS	VN	V	—
Perm	P	Profile	P	Cath	P+TS	VN	V	—
Perm	P	Network	N	URL	P+TS	VN	V	—
Perm	P	System	S	AVC	A+TS	VN	V	—
Join	J	Profile	P	Cath	Z+TS	CORE	C	—
Join	J	Profile	P	Cath	F+TS	CORE	C	—
Join	J	Network	N	URL	L+TS	VN	V	—
Join	J	System	S	PPLL	N+TS	VN	V	—

[0115] As such, the ID packet now provides a method to “point” to a specific row in the database, due to the fact that all of the preambles and the time stamps exist. Although Table 3 illustrated only a single ID in the ID packet, it should be understood that each ID packet is represented by all of the IDs, which comprise a single row in the database. This database is typically populated at the ID server and then the ID server, as described hereinabove, “pushes” all of the ID packets in the database to the respective account servers such as the conversion server, the router, etc. Also as noted hereinabove, some of these ID packets could identify processes. In this situation, it might be that all of the information in the database and an ID server need not be transferred to each and every one of the accounts such as the conversion server and the router. Only the information associated with data packets that would be processed or handled by that particular server would be required at the conversion server, router, for example.



[0116] Referring now to FIGURE 29 there is illustrated a flow chart depicting the operation of entering a profile. The program is initiated at a block 2902 and then proceeds to a block 2904 to enter the profile, this typically performed by a user. It could be that, additionally, a profile that is received in the form of a filled out "form" that is provided by some input device from a non-system user. That is, for example, ordering a product from a system node in a transaction. If the profile already exists, as determined by a decision block 2906, then the program will flow to a function block 2910 to use an existing ID. However, if the ID does not presently exist, the program will flow along a "N" path to a function block 2912 wherein a time stamp will be applied and then to function block 2914 where a sequence number will be assigned. Typically, if this particular device is creating new packets, a different sequence number will be attached to the various time stamp in a predetermined sequence. However, this could be a random sequence. The program then flows to a function block 2916 to store the ID and then to a decision block 2918 to determine if more profiles are to be entered. This is also the destination of the function block 2910. If more are required, the decision block 2918 will flow back to the input of function block 2904 and, if not, the program will flow to an End Block 2920.

[0117] Referring now to FIGURE 30, there is illustrated a diagrammatic view for defining a single ID in an ID packet. This ID is associated with the profile for a butterfly catheter. This typically will be the item ID. There are provided, for example, six fields, the first associated with whether it is a permanent or a joiner ID, defined by a "P" or a "J," a second field associated with whether it is a profile, which is indicated by "P," an item type defining what type the item is, indicated by a word as a user would input it, a fourth field associated with the actual item, *i.e.*, that it is a butterfly catheter (the lowest classification), a fifth field for the overall type of ID packet, this being an "ID" packet, indicated by an "I," indicated by "C" or a "V," respectively, and a sixth field associated with the type of ID it is, an Individual ID, "I" or a Group ID "G."

[0118] In the first profile input, the user indicates it as being a permanent ID, a profile and types out the word "catheter" for the item type, and types and the word "butterfly" of

the item that it is associated with an ID, "J," and that it is an item ID indicated by an "I." The term "catheter" is associated with an alpha letter "C" and the word butterfly is associated with the letter "B." When this is first created, the ID that is generated is "PPCBITS/S." The second item that is entered is identical to the first one in that the user indicated this as being a butterfly catheter. The system will recognize all of the first three and last two classifiers as being identical to others in the system and it will also recognize that the term "butterfly" as identical to a previous one that was entered. This type of search during the classification operation is performed by actually looking at the database in the non-coded column for the particular word in the field. This essentially looks at the spelling of the word. Since the spelling is the same as a previous one and the first three and last two fields are the same, then this will be identical to an ID packet that exists and a new ID packet need not be created. However, suppose a situation occurred where the user misspelled the term "butterfly" as "butterfly." In this situation, the database search would not turn up this misspelling (this is assumed that the system does not have some type of spell check to allow adaptability to this type of situation) which basically determines this as a new item in the database. As such, a new alpha character will be associated with the item field, *i.e.*, the fourth field, which is the alpha character "L" associated with the time stamp and this will comprise a new row in the database. For the last example, suppose that the item that is to be classified as a butterfly catheter with the correct spelling, but that the fifth field is a pulmonary description. In this event, this will be a different ID and may actually result in a different alpha character for the fourth field associated with the item. As illustrated, this can be assigned as an alpha character "P," which may be different, but it uniquely identifies this as a different item associated with a pulmonary catheter. However, it is the time stamp that makes it unique even if the same character is used.

[0119] Referring now to FIGURE 31, there is illustrated a diagram of a system for layering data packets received from different systems that are potentially "non-like" systems. There are illustrated three systems, a system 3102, a system 3104 and a system 3106, labeled system "A," "B" and "C," respectively. Each of these systems operates in a different environment and may actually have a different database structure. For example,

one might utilize an Oracle database with a specific and clearly defined database structure and another system might utilize a different database structure. Each of these database structures is an independent structure with possibly separate methods for identifying vendors and the such, *i.e.*, there can actually be a different vendor number in each system for the same vendor or a different product number for a common product. However, in the overall system utilizing the ID packets, there can only be one common ID for a packet associated with any vendor or item. For example, if a field were present for an employee number associated with an employee, a field present for the days worked and a field present for the days out of the office, each of these particular types of data would be reflected in a different format in each database. Therefore, a specific employee number from one database would have to be converted into an ID packet format for the master system such that both systems employee number could be recognized, categorized and analyzed, or transferred from one system to the other.

**[0120]** The manner for converting data and information in one database to the master system is provided by the extensions referred to hereinabove as "Extents," that provide a software program for retrieving information from the non-master database and converting it to ID packets from the master system. System 3102 has associated therewith an Extent 3108, system 3104 has an Extent 3110 associated therewith and system 3106 has an Extent 3112 associated therewith. Each of the Extents 3108 is operable to retrieve the data and forward it to a conversion server 3114 as ID packets. The interface connection between the Extents 3108-3112 and the conversion server 3114 are illustrated as separate connections, but they are actually transferred through the network. Additionally, there could be multiple inputs to the conversion server from different networks.

**[0121]** Each of the Extents is interfaced to an ID server 3116, which ID server 3116, which ID server 3116 is operable to "push" IDs for various items and the such to each of the associated Extents. For example, if system 3102 had associated therewith database information that was to be converted over to an ID packet out of the ID packets associated therewith would be stored in the Extent 3108. When initially set up, system 3102 would

recognize for example, that each employee in its database required a separate ID packet to uniquely identify that employee. These would be set up by the ID server 3116 and pushed to the appropriate Extent 3108. Therefore, whenever system 3102 transferred an employee number as part of a data transfer to the conversion server 3114 or any other account server on the system, it would be processed through the Extent 3108 and the appropriate ID packet generated, *i.e.*, extracted from the associated ID packet table of the Extent 3108, and then forwarded to the conversion server 3114. In the example of FIGURE 31, the conversion server 3114 is illustrated as the destination of the information for the purpose of layering, as will be described hereinbelow. However, it should be understood that all of the data will first go to a router and then to the appropriate account server, if necessary. The illustration of FIGURE 31 is simplified for this example.

**[0122]** When data from system A is received for a particular conversion operation, it is stored in a database 3118 in a first location 3120. All the data from system 3104 is associated with a location 3122 and all the information from system 3106 is associated with a location 3124 in database 3118. This information is layered, such that common ID packet types, such as employee numbers, are arranged in a predetermined format. This is illustrated in a Table 3126, which is organized to illustrate four ID packets, IDP1, IDP2, IDP3 and IDP4. IDP1 may be employee numbers which are arranged in three locations, such that they all are in a common column. It should be understood that each of the IDPs can be different for employee numbers, *i.e.*, each employee has a separate distinct ID packet. As such, if system 3102 and system 3106 both had the same employee in their database, they would have a common ID packet associated with the ID server 3116, this being set up initially. It can be seen, therefore, that the layering system allows a transaction or an analysis to pull data from non-like systems, convert it to like data in an organized structure and dispose it in a common table that will allow analysis thereof. An example of this will be described hereinbelow.

**[0123]** Referring now to FIGURE 32, there is illustrated a diagrammatic view of the transaction system for utilizing ID packets to converse between two systems through a

master space. As described hereinabove, this master space includes the router, the network mesh, the core servers, the ID server, etc. that are required to process data packets. In FIGURE 32, this system is illustrated with a block 3202 that defines the master data system. The master data system is essentially a system that receives, routes and operates on data packets to perform processes, etc. As described hereinabove, each of these ID packets constitutes a pointer to some process associated with traversal of information through the master data system 3202 from an origination point outside the system to a destination point outside the system through the master data system 3202 or to a point within the master data system for processing thereof. This processing system is referred to with a block 3204 which is operable that is also provided a master ID server 3206 that contains the ID packets that are operable with the system, these referred to as internal ID packets. These are differentiated from external ID packets for an external system, which is not disclosed herein.

[0124] There is provided an external system 3208 that interfaces with the master data system 3202 via a conversion block 3310, system 3308 having a local database 3312 that is associated with its native database language or structure. Similarly, there is provided a second system 3314 that is interfaced with the master data system through a conversion block 3316 and has associated therewith a native database 3318. In order for system 3308 to interface with system 3314, it is necessary to extract data, convert it to an ID packet that is compatible with a master data system 3202, process it therein and then route it to system 3314 through the conversion block 3316, at which time it arrives at system 3314 in a structure similar to the native database 3318. This allows non-like systems to communicate with each other as long as they have a common space to go through.

[0125] In order to operate in this manner, there must be some type of conversion to the master data space. This is not necessarily defined by the system itself, but, rather, the master data system 3202 through its ID server 3206 defines the manner by which each system will communicate therethrough. As such, this is a push operation with the definition. Not only are the parameters of the definition assigned, but the actual ID packet

that is communicating therebetween. For example, there may actually be a common item, such as a catheter, that exists in both databases. By having this information determined by the master ID server 3206, an ID packet can be generated in the master ID server 3206 and associated with the same items in the two different databases 3312 and 3218. As such, it is important that the master ID server be able to identify the ID packet and associate it with the same item in two different databases such that, when pushing the ID packet to one of the systems, it also pushes the associated relationship to information in the database 3312 or 3318. For example, an employee number in database 3312 has a certain format and value that is set up in the master ID server 3206 as being related to a specific ID packet. When the ID packet is transferred to the conversion block 3310, it is associated with its value in the database 3312. Therefore, whenever the value in database 3312 is sent to the conversion block 3310, this value acts as a pointer and the appropriate ID packet can then be forwarded to the master data system 3202.

**[0126]** Referring now to FIGURE 33, there is illustrated an alternate embodiment of the embodiment of FIGURE 32. In this system, there are provided two systems, a system 3302 and a system 3304. System 3302 has associated therewith a master data system 3306 and a master ID server 3308. System 3304 has associated therewith a master data system 3310 and a master ID server 3312. There is provided one external system, system 3314 associated with system 3302 in a conversion block 3316 disposed between system 3314 and master data system 3306. There is associated in a local database 3318 with system 3314. ID server 3308 is internal to the master data system 3306. Therefore, whenever system 3314, which is part of system 3302, communicates with master data system 3306, it will use internal ID packets associated with the ID server 3308, as described hereinabove. However, when conversing with master data system 3310, the ID packets are different, they are those associated with ID server 3312, these being external to system 3302. Therefore, master data system 3306 has stored in ID server 3308 external ID packets associated with the external side of the system, *i.e.*, all other systems that are external thereto.

[0127] System 3304 has associated therewith an external system node 3320, which communicates with master data system 3310 through a conversion block 3322 and also has associated therewith a local database 3324.

[0128] When a transaction occurs which requires information to be transmitted from system 3314 over to system 3320, a data packet will be generated for information in the local database 3318. For example, if a simple transaction such as an employee number was required to be transferred to system 3320 for operations thereon as a portion of a process, the employee number would be extracted from D database 3318 with the conversion block 3316, as part of the overall transaction. This employee number would be converted to an internal ID packet associated with system 3302. At the master data system 3306, information in the ID server 3308 would be utilized to determine the external data packet to be transferred to master data system 3310. As described hereinabove, it could actually be the ID packet associated with the employee number that resides in ID server 3312. Alternatively, it could be a joiner ID packet which is a negotiated ID packet between the two systems, such that the actual ID packet associated with the employee number in either of the systems 3302 or 3304 is not known to the other.

[0129] Once the ID packet, with a joiner ID packet, are transferred from master data system 3306 to master data system 3310, it is the processed in accordance with the transaction and transferred to the conversion block 3322 as the appropriate ID packet for that employee number. This is then converted to the format of database 3324 and processed by system 3320.

[0130] Referring now to FIGURE 34, there is illustrated a diagrammatic view of an example of a transaction. In this transaction, it is desirable to have information about employees as to the number of days they worked and the number of days they did not work. This information is analyzed in the master data system 3202. Therefore, the first thing that must be performed is a conversion from the employee number to a data packet, the days in information to a data packet and the days out information to a data packet. The

employee number has previously been determined through a profiling operation to be defined as a unique ID packet. Therefore, a relational database can be utilized to pull the employee number from a database that is associated with the conversion block. The days in information can also be a unique data packet. For example, there could be a unique data packet for the days in information for values from 1-364, each different. Alternatively, there can be a single ID packet associated with the days in field and then a collateral or ancillary value data field that could be transmitted after the ID packet, as described hereinabove with respect to variable length data. This is the same situation with the days out field.

[0131] The information is illustrated in a table 3402 in the native database. This is converted to a packetized value for a given row in a transaction packet. The first ID packet, IDPKT P, 3404 is generated to indicate the process that is being carried out, *i.e.*, employee information regarding the days in and days out as being transferred to the master data system 3202 for the purpose of evaluating information in a particular process. This is followed by an ID packet 3406 labeled "IDPKT EM" for the employee number. Followed by that would be an ID packet 3408 for the days in. This is followed by an ID packet 3412 for the days out information. At the end of the information is provided a termination data packet 3418. This represents a single row of information being transferred, although it should be understood that the initiation of the process could constitute multiple rows and information in the form of an ID packet could be forwarded as a part of the transaction packet indicating the block size of the data that would be sent. This is then "stacked" in a stack 3420 such that it is stacked in a processing string as opposed to an organized data structure of columns and rows. Since the data is comprised of data packets, it is possible to place the data in such an organization.

[0132] Referring now to FIGURE 34A, there is illustrated a diagrammatic view of how the database is populated with ID packets. It can be seen that there are two columns, one for employee and one for an ID packet that represents data in and data out. It can be seen that unlike data is stored in the second column, *i.e.*, that the information regarding days in



is different than that regarding days out in that it would normally be contained within different columns of a database. This facilitates the processing operation. Therefore, by utilizing ID packets, the ID packets can be assembled in single columns representing different data. Further, they can be assembled in the column in the sequence in which information is to be processed in the later analysis routine.

**[0133]** Although the preferred embodiment has been described in detail, it should be understood that various changes, substitutions and alterations can be made therein without departing from the spirit and scope of the invention as defined by the appended claims.

09443674360